

## Cybersecurity in 2023 and beyond: 12 leaders share their forecasts

What obstacles and opportunities might be in store for your organization? These 2023 forecasts from leaders at the cyber front lines reveal a range of insights and strategies, from greater emphasis on future forward readiness to the increased role organizational resilience will play in controlling exposure to threats and managing multifaceted risks.



### Brand trust will be built on data-centric security

"There is growing urgency for organizations to embrace data privacy, security, and compliance as mechanisms to bolster customer experience, trust, and brand perception."

**Criss Bradbury**  
Cyber Markets, Offerings, and Alliances Leader,  
Deloitte & Touche LLP



### Security will be a critical enabler in the adoption of emerging tech

"The sustained success of IoT, Blockchain, 5G, Quantum, and other applications will largely be based on the ability to navigate and implement appropriate cybersecurity technology measures in tandem with adoption."

**Kieran Norton**  
Transformation & Emerging  
Technology Market Leader,  
Deloitte & Touche LLP



### Organizations can build agility with future-ready cyber tech

"Breakthrough cyber tech, including AI, will lead to a more proactive risk approach as well as greater innovation, competitive differentiation, and operational excellence. Organizations need to actively build a unified cyber strategy to be agile enough to seize future opportunities before they emerge."

**Deborah Golden**  
Chief Innovation Officer,  
Deloitte & Touche LLP



### The shift-left movement will improve application security

"Developers won't be working in isolation; security improvements will be embedded in the process of application creation throughout the process from development to production."

**Asheem Chandna**  
Investor and Company Builder,  
Greylock Partners



### Comprehensive supply chain security is imperative

"Supply chain threats continue to evolve in complexity, requiring a greater focus on deploying and operating identity and access management (IAM) and Zero Trust capabilities to enforce authorized third-party access."

**Sharon Chand**  
Cyber & Strategic Risk Ecosystems  
& Alliances Leader,  
Deloitte & Touche LLP



### Proliferating cloud services create new possibilities and risks

"The huge shift to cloud-based data and business functions has created unprecedented possibilities—but comes with costly regulatory missteps and damaging cyberattacks when security is not woven into the process. Organizations can enable agile, secure transformation by leveraging "secure-by-design" processes and Zero Trust principles."

**Vikram Kunchala**  
Cyber & Strategic Risk Solutions Leader,  
Deloitte & Touche LLP



### Humans can't do it alone

"The combination of ongoing talent shortages and increasing efforts from adversaries makes automation critical. Humans just can't respond fast enough. Software is needed to fight software—for detection, response, and prevention."

**Jay Leek**  
Managing Partner & Co-founder,  
SYN Ventures



### Machines can't do it alone, either

"If you automate a bad process, you're just running yourself off a cliff. You still need process best practices and people to oversee it."

**Ken Gonzalez**  
Managing Director,  
NightDragon Investments & Advisory



### Focus on organizational resilience will continue to grow

"The multitude of supply chain, geopolitical, environmental and cyber disruptions are challenging traditional risk programs. An integrated view of risks can help lead organizations to employ new techniques and technologies to improve threat awareness and response."

**Pete Renneker**  
Technical Resilience Leader,  
Deloitte & Touche LLP



### Growing talent shortages and labor costs will lead to cyber talent consolidation and outsourcing

"With cybersecurity risks and regulations increasing by the day, many organizations are scrambling to fill positions. To stay agile, they'll need to focus on hiring niche cyber talent along with outsourcing strategies."

**Deborah Golden**  
Chief Innovation Officer,  
Deloitte & Touche LLP



### Device visibility and security will be a major area of focus

"As the number of IoT-connected devices grows, the attack surface grows with it. Leading organizations will need to increase their focus on device policies, procedures, and inventories, as well as closer monitoring of those devices."

**Wendy Frank**  
Cyber IoT Leader,  
Deloitte & Touche LLP



### Threats to operational technologies will continue to evolve rapidly

"Operational technology (OT) environments are increasingly being weaponized. This is prompting greater visibility into OT devices, networks, and an increase in monitoring tools to better correlate security of OT and IT networks."

**Ramsey Hajj**  
Cyber OT Leader,  
Deloitte & Touche LLP



### Boards will increasingly view cyber readiness as a business imperative

"The role that the board plays in cyber oversight is becoming more important, as is their ability to position cyber as a strategic enabler across customer, vendor, employee, and shareholder relationships."

**Mary Galligan**  
Crisis Management Leader,  
Deloitte & Touche LLP



### Companies will drive innovation to solve global issues

"There's a shared sense of corporate social responsibility—a mission to protect our way of life, governments, families, and corporations—that's driving new innovations."

**Ken Gonzalez**  
Managing Director,  
NightDragon Investments & Advisory



### Expanding attack surfaces will be secured through increased automation

"With the expanding threat surface becoming more complex for most organizations, there is a tremendous opportunity to leverage APIs that can improve automated threat detection using AI and ML."

**Asheem Chandna**  
Investor and Company Builder,  
Greylock Partners



### Geopolitics will make the attack surface more complicated

"On the attack side, threats aren't just from individual bad actors, but also nation states. It will be very hard for organizations to manage threat protection themselves, as these attacks have high levels of sophistication."

**Asheem Chandna**  
Investor and Company Builder,  
Greylock Partners

For the challenges you can't predict, and the opportunities you can't pass up

While the stakes are high for addressing the complex cyber and risk challenges of 2023 and beyond, Deloitte can help you meet your objectives, whether you need assistance with strategy, design, implementation, or ongoing operations. We offer a unified approach to help you tackle obstacles, build new capabilities, and move forward fast—wherever you are on your journey.

Learn more at [Deloitte.com/us/MoveForwardFast](https://www.deloitte.com/us/MoveForwardFast)